MNE7 Access to the Global Commons Outcome 3 Cyber Domain

Framework of Processes to Support the Generation and Maintenance of Cyber Situational Awareness Within the Global Commons

Version 1.0
Dated 28 Feb 2013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 JUL 2013	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
MNE7 Access to the Global Commons Outcome 3 Cyber Domain Framework of Processes to Support the Generation and Maintenance of Cyber Situational Awareness Within the Global Commons Version 1.0 Dated 28 Feb 2013	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
Nations and organisations require concepts and capabilities for anticipating, deterring, preventing, protecting against and responding to a disruption or a denial of access to the global commons domains (air, maritime, space and cyber) and for ensuring freedom of action within them, while taking into account their interrelationships.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**6**	

MULTI-NATIONAL EXPERIMENT 7
ACCESS TO THE GLOBAL COMMONS
Cyber Domain Outcome 3 & Objective 3.5

MNE7 Problem Statement	Nations and organisations require concepts and capabilities for anticipating, deterring, preventing, protecting against and responding to a disruption or a denial of access to the global commons domains (air, maritime, space and cyber) and for ensuring freedom of action within them, while taking into account their interrelationships.
Outcome 3	Decision makers can gain sufficient understanding (including legal) and situational awareness of their own networks and relevant parts of wider cyberspace, drawing upon integrated and collaborative information, improving their ability to make timely, informed and effective decisions on the actions that allow us to anticipate, deter, prevent, protect, respond and rapidly affect an adversary's ability to disrupt or degrade our access to and freedom of action within the global commons.
Objective 3.5	Develop a framework for gaining and maintaining collaborative and integrated situational awareness.
Scope	The scope of Objective 3.5 cyber domain situational awareness is to retain a broad concepts development and experimentation approach that encompasses international, national and military aspects, primarily focused at the strategic level, whilst recognizing the blurring of the strategic, operational and tactical levels of decision-making.

Framework of Processes to Support the Generation of Cyber Situational Awareness

Reference:

A. MNE 7 Campaign Lexicon, draft version 4, dated 28 November 2011.

BACKGROUND

There is currently a gap in our ability to gain sufficient situational awareness and understanding of the cyber domain at the national and international level. All domains have a dependency on cyberspace and cyber SA should provide the underpinning confidence to carry out activities in those domains.

There are two levels to cyber SA:

> The first is visibility of the current **cyber status** of an individual, organisation, multinational corporation or nation based on an understanding of indentified threats and the adoption of solutions/protection to them.
>
> The second is based on accepting that in cyberspace it is impossible to prevent, or even predict all attacks – a new/previously unseen, 'attack' will happen to someone, somewhere (zero day attack). If the one who is attacked shares appropriate information about the attack as soon as possible, others may have more time in which to implement some form of mitigation.

The first could be considered as 'good housekeeping' – maintaining up-to-date anti-virus programmes and adopting 'patches' in a timely manner.

The second is somewhat more altruistic in approach – '*My detection = Your protection'*. It is dependant on the information shared being sufficiently relevant to a recipient, for the recipient to understand that he may have a problem and the provenance is such that he can act on it.

AIM

To provide a common framework of processes based on the Outcome 3 work that supports the generation of cyber situational awareness that will enhance the ability of decision makers to take those decisions to maintain the operation/capability/service for which they are responsible, in good time.

DEFINITIONS

There is no single agreed lexicon or taxonomy that supports cyber domain situational awareness across governments, agencies, allies, industry and academia. Multinational Experiment 7 (MNE7) has therefore produced a Campaign Lexicon (Reference A).

COLLABORATIVE CYBER SITUATIONAL AWARENESS (CCSA)

CCSA is dependant on information being collected, analysed and the output fused into an output from which the decision maker can easily assess the impact of 'an event' on his/her area of responsibility. In addition the decision maker must have sufficient confidence in the information presented and understanding of the potential legal issues to allow him/her to take the appropriate action.

These aspects are covered by each of the Outcome Objectives – 3.1, 3.2, 3.3 and 3.4. In each case a very brief overview is given of the Objective and a link to the specific products. The background thinking behind the issues that each Objective is designed to support or overcome can be found in the **CONEMP**.

The starting point is the sharing of information, which immediately raises issues of **trust**, the ability to **understand** the information shared and a cost/benefit analysis as to the **benefit** of sharing the information. The intent is that information is shared 'one-to many' not simply one-to-one; there is no assumption of knowledge about what information is of value to another.

Objective 3.2 The Information Sharing Framework (ISF) provides guidance on how to establish the capability to increase an organisation's cyber Situational Awareness (SA) enabled by sharing information across a trusted community of interest. It describes the context and the business case for participation, and includes the collaborative governance, federated access control and management of information quality. All of which are required for effective decision making.

To achieve the maximum warning time it is desirable that information sharing goes beyond single communities of interest and spans many both nationally and internationally. CCSA is dependent on **cross-sector and multinational** information sharing.

For the shared information to be of value to the recipient, the recipient must understand its relevance to him/her – what are their **critical assets** and how are they **dependant on cyberspace.**

Most nations already have an understanding of their own critical infrastructures and assets, but there is an increasing realisation of the extent to which those infrastructures have a dependency on cyberspace. **Objective 3.1** provides a suggested methodology to enhance resilience in the event of a cyber incident; importantly it provides a means of prioritising the resources available to do so.

Equally important to achieving CCSA is the manner in which the information is presented to the decision makers. It must be in a context that is relevant and enables a high level decision maker to rapidly identify the likely impact of any event. **Objective 3.4** and the **Outcome LOE** considered enabling technologies that support the fusion and presentation of information to provide CCSA.

Finally ensuring a legal response to any 'cyber incident' is not simple; whilst conventions and agreements exist at the national/regional level there is no commonly shared international legal framework. **Objective 3.3** provides decision makers with a tool to

support their understanding of the (international) legal implications that underpin any response options to a cyber incident.

CCSA IN CONTEXT

As with all domains cyber situational awareness not only provides visibility of the 'health' of that domain but contributes to the wider, global situational awareness picture (Figure 1). However to be of value the information from cyber SA must be trusted and as the newest domain, cyber is still building that trust as understanding of the domain evolves. The 'Framework of Processes' provides guidance on how trust in CCSA can be achieved now and further developed in the future.

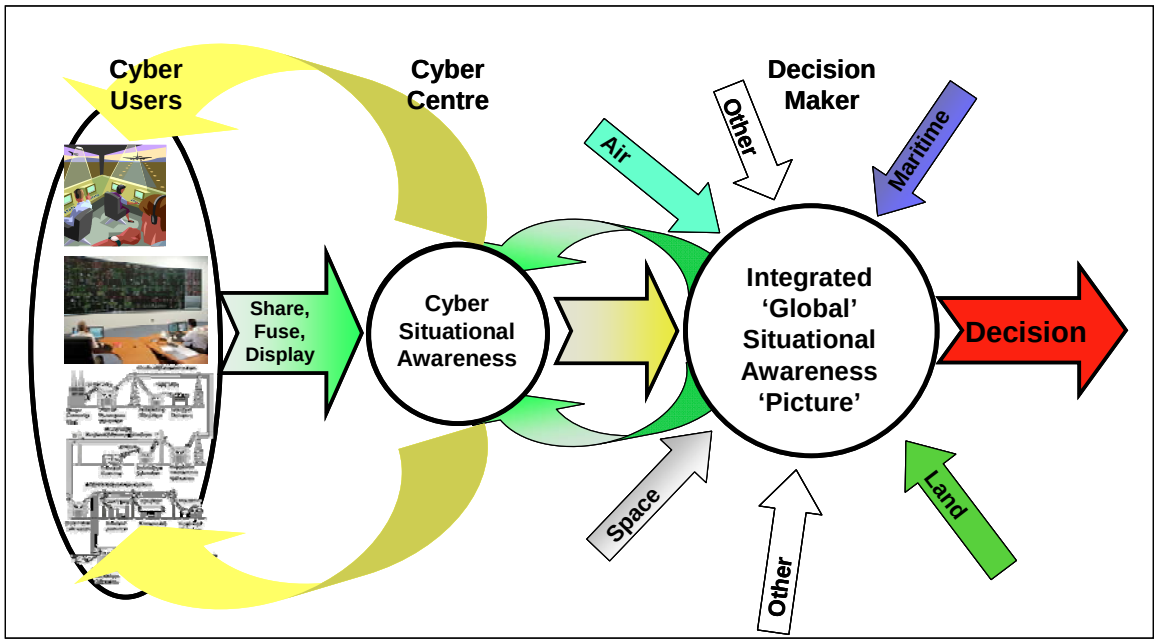

Figure 1: Cyber Situational Awareness in Context

FRAMEWORK OF PROCESSES

At the start of the MNE 7 process it was felt that a 'Framework of Processes' to support the generation of CCSA would be a suitable way of summarising the activities and capabilities required. It appears a little simplistic as a 'product' in its own right but together with the outputs from each of the Objectives should provide direction for the allocation of resources based on a review of dependencies on cyberspace, a means to generate situational awareness and guidance on the legal requirements pertaining to any follow on action or response. A diagrammatic representation of the Framework of Processes is at Figure 2.

The framework ensures the CCSA generated is of sufficient quality (timeliness, accuracy and richness) and reliability to be of genuine value to decision makers when presented in context / as part of a 'global' common operating picture.

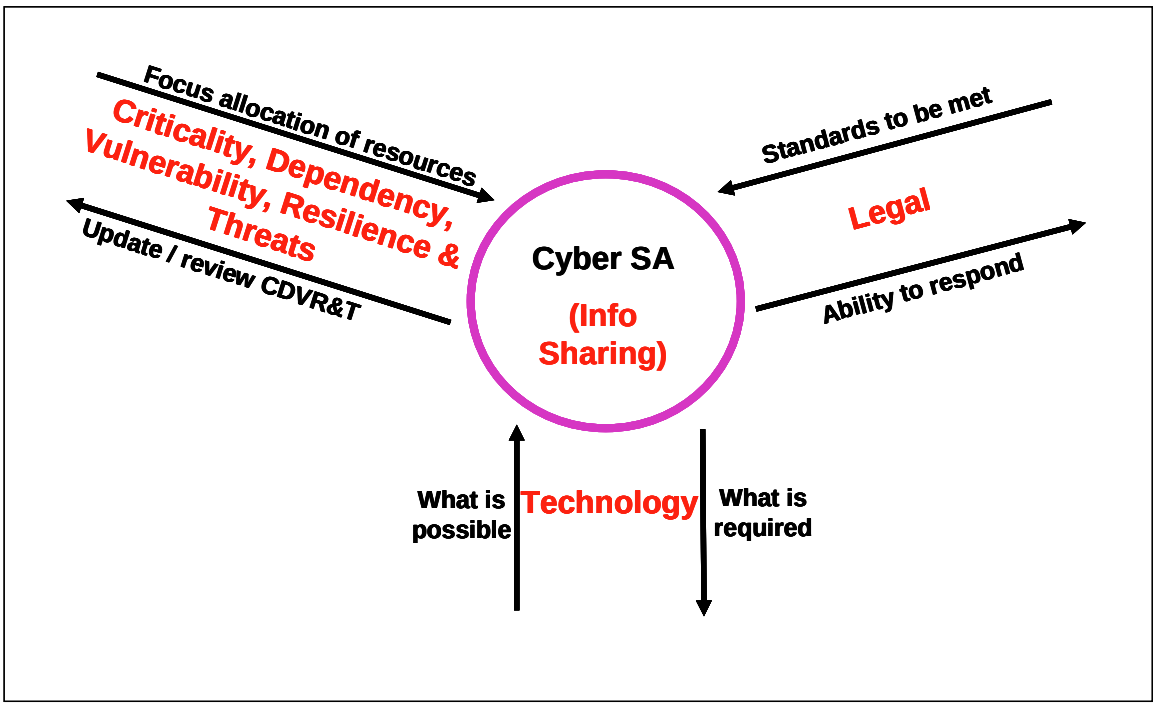

Figure 2. Framework Of Processes